SANS The most trusted source for information security training, certification, and research

GIAC CERTIFICATIONS

OnDemand

Simulcast

vLive

ONLINE CYBERSECURITY TRAINING

Rewind | Revisit | Reinforce | Retain

> “I love the material, I love the SANS Online delivery, and I want the entire industry to take these courses.” —NICK SEWELL, IIT

Exclusive Special Offers
Choose a **tablet**, **laptop**, or **course discount** offer with select OnDemand and vLive courses. For more details, visit **sans.org/online**

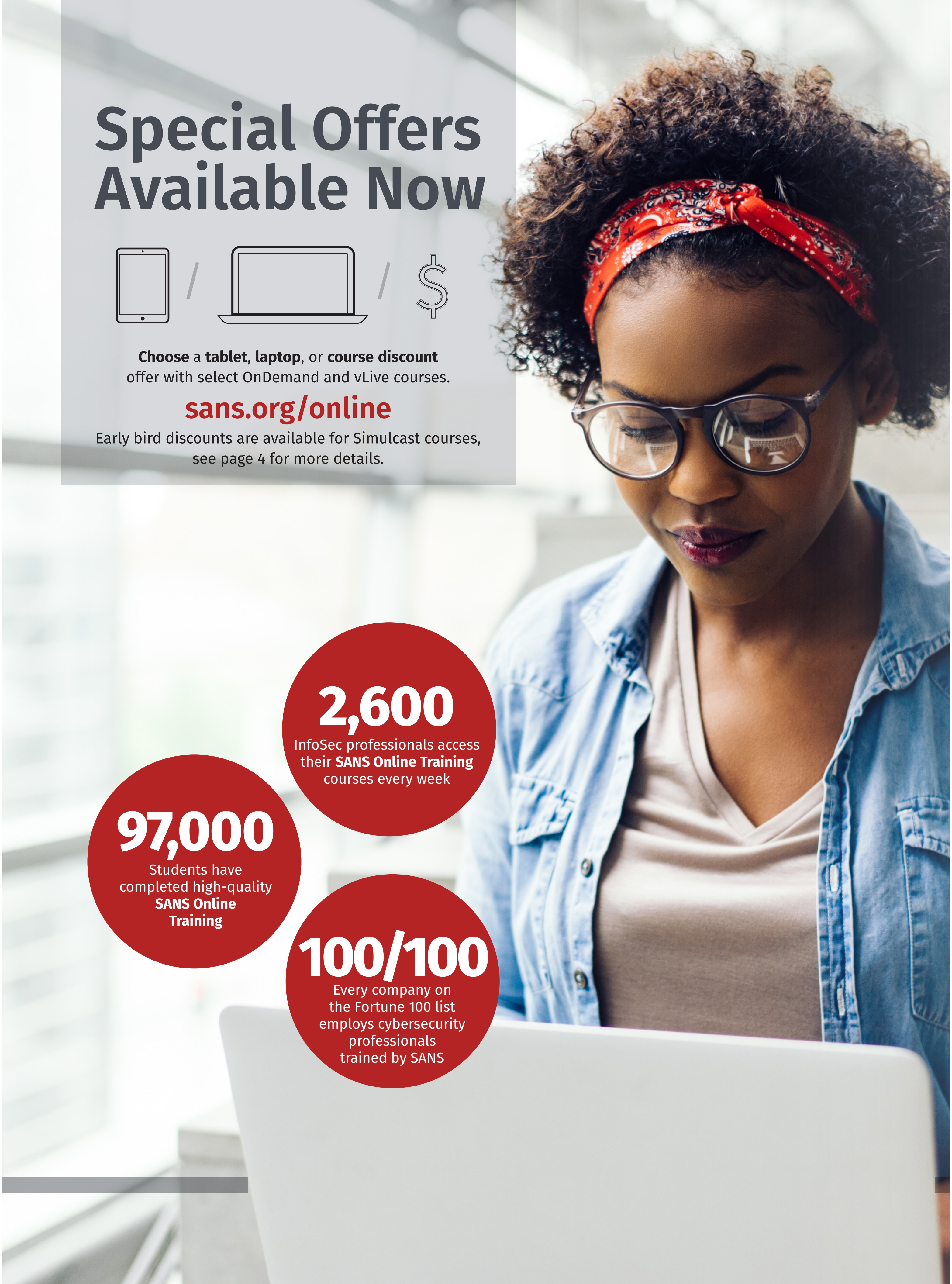
FALL 2019 COURSE CATALOG

Special Offers Available Now

Choose a **tablet**, **laptop**, or **course discount** offer with select OnDemand and vLive courses.

sans.org/online

Early bird discounts are available for Simulcast courses, see page 4 for more details.



2,600

InfoSec professionals access their **SANS Online Training** courses every week

97,000

Students have completed high-quality **SANS Online Training**

100/100

Every company on the Fortune 100 list employs cybersecurity professionals trained by SANS

SANS ONLINE TRAINING

OnDemand

Train at your own pace anytime, anywhere

Simulcast

Stream live SANS training to your home or office

vLive

Train live in the evenings online, from anywhere

SelfStudy

Train with flexibility and on your own schedule

> **"I love the flexibility that SANS Online Training offers, and being able to review and revisit content has helped me translate new skills into new work products."**
>
> **—WILLIAM AMURGIS, Baycare**

About SANS Training & GIAC Certifications

Cybersecurity professionals around the world turn to the SANS Institute and GIAC Certifications for the most trusted hands-on cybersecurity education available. From security awareness to small group training and large, live events, and from online training to team challenges, skill assessments, certifications, and degrees, the SANS mission is to advance the cybersecurity skills of as many professionals as possible to protect our society.

Inside This Catalog

This training guide and the enclosed IT Security Course Roadmap will help you plan your education and accelerate your career! The roadmap pullout contains all of the job role, development path, course, and certification information needed to pursue the career you want in cyber defense, penetration testing, digital forensics and incident response, management, or secure development.

You'll find the roadmap between pages 10 and 11.

TABLE OF CONTENTS

> “The OnDemand platform couldn’t have been more convenient – having four months to complete my course allowed me to balance work, life, and training well.”
>
> —JILL FRASER, JEFFCO

ONDEMAND

Train at your own pace anytime, anywhere.

Why Students Choose SANS OnDemand

- Four Months of Access to Comprehensive Online Training, Virtual Labs and Quizzes
- Converse with GIAC-Certified Subject-Matter Experts
- Web-Based Training Accessible 24/7 from Your Desktop, Laptop, iPad, or Android Tablet
- No Travel or Time Away from the Office
- Includes Video, Labs, and Hands-On Exercises
- Complete Set of Books and Course Media
- Course Progress Reports
- More than 45 Courses Available – Anytime, Anywhere
- Perfect Preparation Tool for the GIAC Exam

SANS ONLINE TRAINING

More than 45 of SANS most popular information security courses are available via OnDemand, our proprietary online training platform. With four months of digital access to your course, quizzes, and labs, plus all of the corresponding printed books and materials, you’ll have plenty of time and resources to master your course content.

If you lack a travel budget or simply appreciate having extended, fully supported access while training, OnDemand may be the best SANS training option for you.

The benefits of taking your SANS training via OnDemand include:

- Instruction directly from course authors means you will receive the best information security training available
- Live chat with GIAC-certified subject-matter experts gives you quick answers to questions and help with complex topics
- Rewind, fast forward, and pause options give you total control over the pace of your course
- Progress tracking and quizzes keep you focused on achievement and content retention
- Search, bookmark, and note-taking options let you highlight sections you want to review or include in a study index
- Extended course access is perfect to prepare for GIAC Certification

New features in OnDemand:

- Closed Captioning
- Section Confidence Markers
- Video Pan/Zoom
- Adjustable Panel Sizing
- Course Progress Bar
- Dynamic Jump Back Button
- Take, Export, and Print Your Own Notes
- Adjustable Font Sizing
- Enhanced Keyboard Shortcuts and Accessibility Features

/ / $

Limited time SANS Online Training specials
Options include tablets, laptops, or discounts.
For more information visit sans.org/online

sans.org/ondemand
support@sans.org
301-654-SANS (7267)

OnDemand | Course List

	Cyber Defense	Taught By
	SEC301: Introduction to Cyber Security | GISF	Keith Palmgren
	SEC401: Security Essentials Bootcamp Style | GSEC	Bryan Simon
NEW!	**SEC402:** Cybersecurity Writing: Hack the Reader	Lenny Zeltser
	SEC440: Critical Security Controls: Planning, Implementing, and Auditing	Randy Marchany
NEW!	**SEC450:** SEC450: Blue Team Fundamentals - Security Operations and Analysis	John Hubbard
	SEC455: SIEM Design & Implementation	Justin Henderson & John Hubbard
	SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis	Micah Hoffman
	SEC501: Advanced Security Essentials – Enterprise Defender | GCED	Stephen Sims
	SEC503: Intrusion Detection In-Depth | GCIA	David Hoelzer
	SEC505: Securing Windows and PowerShell Automation | GCWN	Jason Fossen
	SEC506: Securing Linux/Unix | GCUX	Hal Pomeranz
	SEC511: Continuous Monitoring and Security Operations | GMON	Eric Conrad
	SEC530: Defensible Security Architecture | GDSA	Justin Henderson and Ismael Valenzuela
	SEC545: Cloud Security Architecture and Operations	Dave Shackleford
	SEC555: SIEM with Tactical Analytics| GCDA	Justin Henderson
	SEC566: Implementing and Auditing the Critical Security Controls – In-Depth | GCCC	James Tarala
	SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses | GDAT	Erik Van Buggenhout

	Penetration Testing	
NEW!	**SEC460:** Enterprise Threat and Vulnerability Assessment| GEVA	Matt Toussain
	SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling | GCIH	John Strand
	SEC542: Web App Penetration Testing and Ethical Hacking | GWAPT	Eric Conrad
	SEC560: Network Penetration Testing and Ethical Hacking | GPEN	Tim Medin
	SEC573: Automating Information Security with Python | GPYC	Mark Baggett
	SEC575: Mobile Device Security and Ethical Hacking | GMOB	Joshua Wright
NEW!	**SEC580:** Metasploit Kung Fu for Enterprise Pen Testing	Jeff McJunkin
	SEC617: Wireless Penetration Testing and Ethical Hacking | GAWN	Larry Pesce
	SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	Adrien de Beaupre
	SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GXPN	Stephen Sims

	Digital Forensics & Incident Response	
NEW!	**FOR498**: Battlefield Forensics & Data Acquisition	Eric Zimmerman
	FOR500: Windows Forensic Analysis | GCFE	Rob Lee
	FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics | GCFA	Rob Lee
	FOR518: Mac and iOS Forensic Analysis and Incident Response	Sarah Edwards
	FOR526: Advanced Memory Forensics & Threat Detection	Alissa Torres
	FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response | GNFA	Philip Hagen
	FOR578: Cyber Threat Intelligence | GCTI	Robert M. Lee
	FOR585: Smartphone Forensic Analysis In-Depth | GASF	Heather Mahalik
	FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques | GREM	Lenny Zeltser

	Security Management	
	MGT414: SANS Training Program for CISSP® Certification | GISP	Eric Conrad and Seth Misenar
	MGT433: SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program	Lance Spitzner
	MGT512: Security Leadership Essentials for Managers | GSLC	Frank Kim
	MGT514: IT Security Strategic Planning, Policy, and Leadership | GSTRT	Frank Kim

	Audit	
	AUD507: Auditing & Monitoring Networks, Perimeters, and Systems | GSNA	Clay Risenhoover

	Legal	
	LEG523: Law of Data Security and Investigations | GLEG	Benjamin Wright

	DevSecOps	
	DEV522: Defending Web Applications Security Essentials | GWEB	Jason Lam
	SEC534: Secure DevOps: A Practical Introduction	Eric Johnson
	SEC540: Cloud Security and DevOps Automation | GCSA	Eric Johnson

	Industrial Control Systems	
	ICS410: ICS/SCADA Security Essentials | GICSP	Justin Searle
	ICS515: ICS Active Defense and Incident Response | GRID	Robert M. Lee

> "I'm at home taking the Online Simulcast class but I feel like I'm there in the room. I don't feel isolated at all. I just have access to my comforts while taking the class."
>
> —DEONA VASTINE, STATE OF CALIFORNIA

SIMULCAST

Stream live SANS training to your home or office.

Why Students Choose SANS Simulcast

- Complete a Course in One Week
- Access Live Training Remotely via the Virtual Classroom
- Four Months of Online Course Access
- Labs, Hands-On Exercises, and Archived Lectures
- GIAC-Certified Subject-Matter-Expert Support
- Complete Set of Books and Course Media
- No Travel Required

Experience live SANS training without traveling by taking your information security course via Simulcast. You'll experience the audio and video feeds streamed directly from the classroom to your laptop, plus real-time interaction with the moderator, peers, and teaching assistants. In addition, you will have access to lecture archives, the online lab environment, and live chat and email support from GIAC-certified subject-matter experts for four months. As a Simulcast student, you will receive the same courseware materials you would receive in a live course, shipped right to your home or office.

All Simulcast courses are recorded and archived, so if you miss part or all of any lessons, or you want to revisit content you will still have four months of access to the archived course content for review.

The benefits of taking your SANS training on the Simulcast platform include:

- Live, scheduled daytime sessions with SANS Certified Instructors
- In-class moderators who actively convey your questions to the instructor and ensure an interactive experience
- Teaching assistants available to support complex content and lab questions during your training sessions
- No travel, which extends training dollars and saves time
- The same instruction and learning outcomes as live training, with an additional four months of online access to revisit and retain the course content

More courses are available, visit **www.sans.org/simulcast** for more information

Austin 2019	Nov 18 - 23, 2019	4 Courses
Pen Test HackFest 2019	Nov 20 - 25, 2019	7 Courses
Cyber Defense Initiative 2019	Dec 12 - 17, 2019	10 Courses
Miami 2020	Jan 13-18, 2020	4 Courses
Las Vegas 2020	Jan 27 - Feb 1, 2020	3 courses
Security East 2020	Feb 3 - 8, 2020	12 Courses

SANS ONLINE TRAINING

$ **Limited time SANS Online Training specials**

EarlyBird course discounts are available for SANS Simulcast courses. Visit **sans.org/simulcast** for more information.

sans.org/simulcast
support@sans.org

> “As always, vLive is the best balance between work, family, and continuing education.”
> —CAMERON DOHERTY, SCE

vLIVE

Train live online in the evenings with SANS top instructors.

vLive is an excellent way to get the best of both worlds – live, interactive SANS training from leading information security practitioners in the comfort of your own home or office. vLive sessions are scheduled in the evening to avoid conflict with your work schedule and feature smaller class sizes that give you an opportunity to connect directly with instructors and peers via the embedded Live Chat Feature. Simply log in at the scheduled times and join your instructor and classmates in an interactive virtual classroom. Don’t worry if you can’t attend every live session; classes are recorded and you can review the class archives for six months.

The benefits of taking your SANS training on the vLive platform include:

- Two conveniently scheduled 3-hour evening sessions (7-10 pm EST) per week over six weeks
- The opportunity to preview content before a session or review content between sessions
- Lecture archives and lab environment available for six months, allowing you to revisit your training for improved retention
- Printed books and materials to facilitate GIAC Certification preparation and testing
- Downloadable MP3s for additional perspectives and experiences
- Access to subject-matter experts via Live Chat and email to get quick answers about complex content or lab questions

Why Students Choose SANS vLive

- Live Evening Courses Taken from the Convenience of Your Home or Office
- Pace of Training Cited as Key Benefit by vLive Student Alumni
- Direct Interaction with Your Instructor and Peers via Interactive Chat Feature
- Six Months of Access to Labs, Hands-on Exercises, and Archived Lectures
- Access to Highly Qualified Subject-Matter Experts

More courses are available, visit **www.sans.org/vlive** for more information

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	Nov 4 - Dec 11, 2019	Moses Frost
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Nov 5 - Dec 19, 2019	Chris Pizor
LEG523: Law of Data Security and Investigations	Nov 11 - Dec 18, 2019	Benjamin Wright
MGT414: SANS Training Program for CISSP®	Dec 2, 2019 - Jan 22, 2020	Tanya Baccam
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Feb 4 - Mar 12, 2020	Chris Pizor
SEC401: Security Essentials Bootcamp Style	Feb 10 - Mar 18, 2018	Tanya Baccam

/ / $

Limited time SANS Online Training specials
Offers include tablets, laptops, or discounts.
For more information visit **sans.org/online**

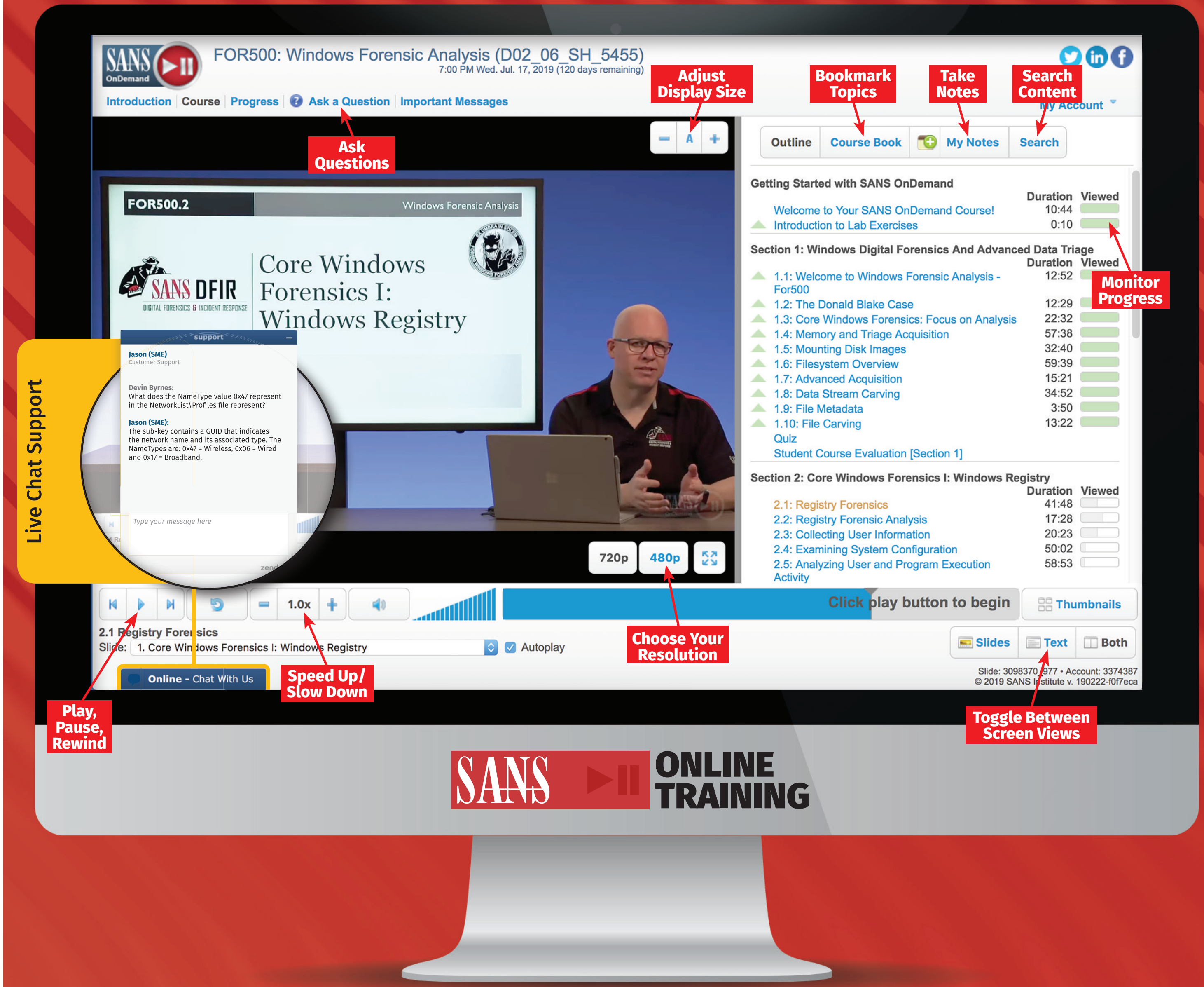
sans.org/vlive
support@sans.org

OnDemand Player

The SANS OnDemand player is custom built to give you control of your training experience.

Below are just a few of the many popular features:

- Closed Captioning
- Section Confidence Markers
- Video Pan/Zoom
- Adjustable Panel Sizing
- Course Progress Bar
- Dynamic Jump Back Button
- Take, Export, and Print Your Own Notes
- Adjustable Font Sizing
- Enhanced Keyboard Shortcuts and Accessibilty Features



Jason (SME)
Customer Support

Devin Byrnes:
What does the NameType value 0x47 represent in the NetworkList\Profiles file represent?

Jason (SME):
The sub-key contains a GUID that indicates the network name and its associated type. The NameTypes are: 0x47 = Wireless, 0x06 = Wired and 0x17 = Broadband.

Getting Started with SANS OnDemand

	Duration	Viewed
Welcome to Your SANS OnDemand Course!	10:44	
Introduction to Lab Exercises	0:10	

Section 1: Windows Digital Forensics And Advanced Data Triage

	Duration	Viewed
1.1: Welcome to Windows Forensic Analysis - For500	12:52	
1.2: The Donald Blake Case	12:29	
1.3: Core Windows Forensics: Focus on Analysis	22:32	
1.4: Memory and Triage Acquisition	57:38	
1.5: Mounting Disk Images	32:40	
1.6: Filesystem Overview	59:39	
1.7: Advanced Acquisition	15:21	
1.8: Data Stream Carving	34:52	
1.9: File Metadata	3:50	
1.10: File Carving	13:22	
Quiz		
Student Course Evaluation [Section 1]		

Section 2: Core Windows Forensics I: Windows Registry

	Duration	Viewed
2.1: Registry Forensics	41:48	
2.2: Registry Forensic Analysis	17:28	
2.3: Collecting User Information	20:23	
2.4: Examining System Configuration	50:02	
2.5: Analyzing User and Program Execution Activity	58:53	

Visit **sans.org/demo** to test drive your next SANS course today

Voucher Program

The SANS Voucher Program is a cybersecurity workforce training management system that allows you to easily procure and manage your organization's training needs.

As a SANS Voucher Program participant, you will be able to:

- Provide your cybersecurity team with the highest standard of skill training and certification available
- Give employees a simple way to select and procure the training they need, when they need it
- Easily approve and manage student enrollment
- Monitor employee training progress and exam scores to ensure satisfactory completion
- Track investments, debits, and account balance for optimal budgeting

Voucher Funds purchased can be applied to any live and online SANS training courses, SANS Summit events, GIAC Certifications, or certification renewals.* Voucher Funds must be used within 12 months, but the term can be extended with additional investments.

Get Started

Visit www.sans.org/vouchers and submit the contact request form to have a SANS representative in your region call or email you within 24 business hours. Within as little time as one week, your eligible team members can begin their training.

*Current exceptions from the SANS Voucher Program are the Partnership program, Security Awareness training, and SANS workshops hosted at events run by other organizations.

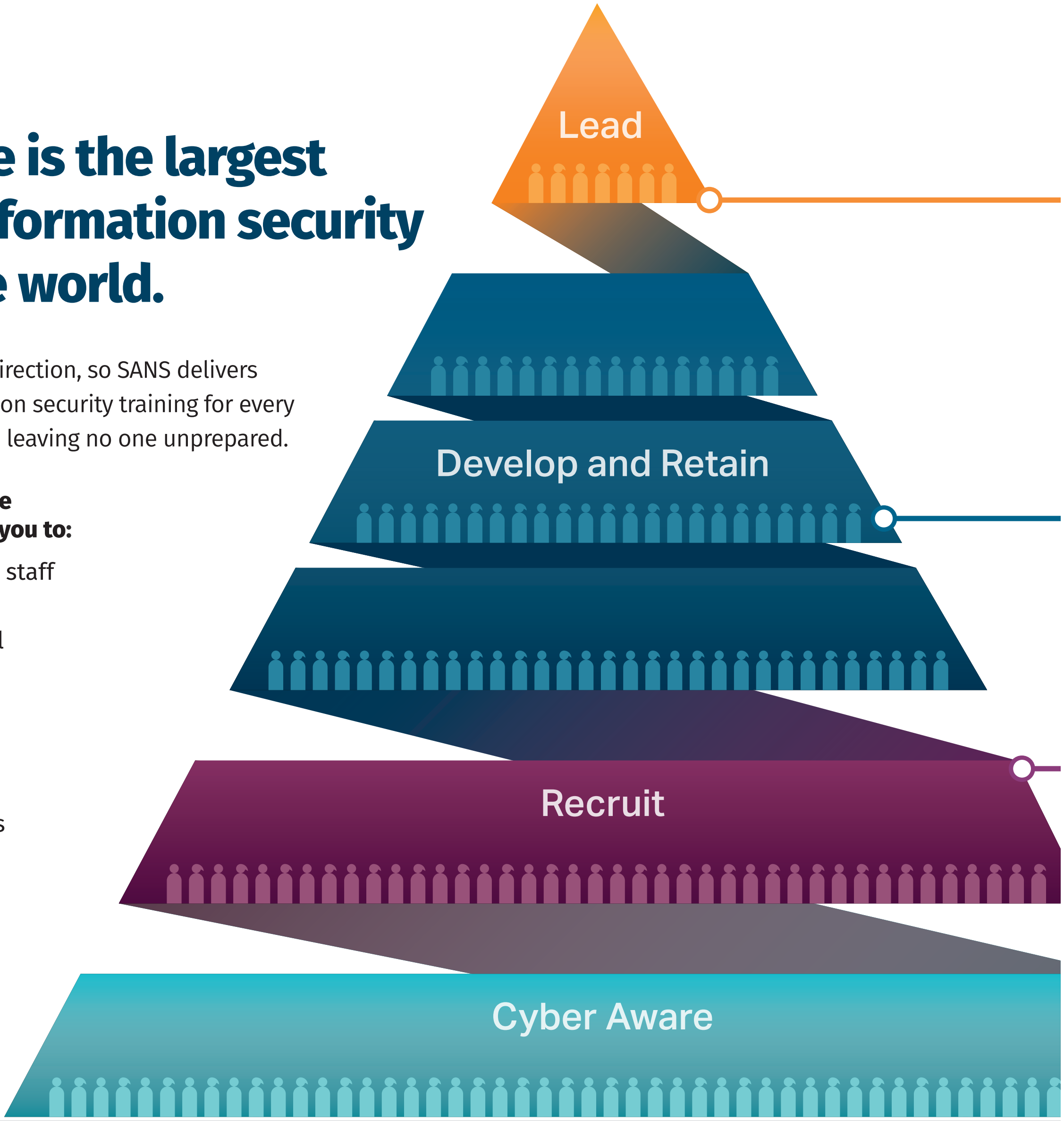
sans.org/vouchers

SANS Institute is the largest provider of information security training in the world.

Threats approach from every direction, so SANS delivers reliable, professional information security training for every member of your organization – leaving no one unprepared.

As a partner in your workforce development, SANS can help you to:

- Arm information security staff with technical standards, techniques, and personal connections to protect your networks and data
- Train non-technical staff to be less susceptible to phishing and web attacks
- Prepare your security leadership to guide your organization towards long-term security



ADDITIONAL WAYS TO TRAIN

Private Training + Simulcast For your dispersed workforce

SANS Private Online Training brings critical information security training directly to your workforce, regardless of their location. Our custom training programs incorporate both live and online instruction, and can be built for almost any SANS course. You'll get a tailored experience built around your specific team's size, location, and composition of learners. And by adding our Simulcast option, your organization can maximize its investment even further.

Private training environments allow students from commercial and government organizations to openly discuss sensitive issues and goals. All courses are led by SANS Certified Instructors; students can ask questions and interact with their instructor and peers during class and labs.

To explore your options for custom, distributed, live, and online workforce training from SANS, contact us at **sans.org/private-training** or email **private-training@sans.org**

Graduate Programs and the GSE

Cybersecurity leadership degrees and elite certification.

SANS Technology Institute

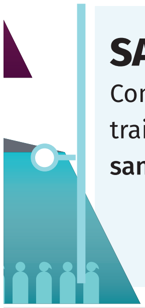
Accredited graduate programs and graduate certificates in information security completed via SANS training.

sans.edu

SANS CyberTalent

Talent assessments, Academies for women, vets, and minorities.

sans.org/cybertalent



SANS Security Awareness

Comprehensive security awareness training tools for all employees.

sans.org/awareness

SANS Training, Certifications, Summits & Cyber Ranges

Proven learning platforms and certifications to advance and validate the skills of information security professionals, offered in live classrooms and online.

Training Events

SANS training events feature our top instructors teaching multiple courses at a single time and location, allowing focused, immersive learning without distractions of an outside environment

sans.org/courses

GIAC

30+ cybersecurity certifications are available in cyber defense, penetration testing, digital forensics, ICS/SCADA and more.

giac.org

Summits

SANS hosts highly focused, expert-led Summits throughout the year that feature presentations and dicsussions on leading issues.

sans.org/cyber-security-summit

NetWars

A suite of live and online hands-on interactive scenario challenges to help you master a wide range of skills.

sans.org/netwars

SelfStudy
For the disciplined InfoSec student

The SANS SelfStudy program is self-paced training for the motivated and disciplined InfoSec student. It's ideal for those who enjoy working independently, can't travel for in-person training, or just prefer an extended study time via course books and MP3s. To learn more or enroll, visit **sans.org/selfstudy**

Courses are now available in:

- Cyber Defense
- Penetration Testing
- Digital Forensics
- Incident Response
- Industrial Control Systems
- Developer
- Audit and Legal

NetWars
Test your cybersecurity know-how

A suite of live and online scenario challenges, SANS NetWars Experiences develop and test your cybersecurity know-how in a safe, interactive environment—all while having a little fun with your fellow IT security professionals.

In NetWars, students develop the real-world skills they'll need to excel in their chosen fields. Participants learn on a cyber range while working through various challenge levels, all hands-on, while mastering the full range of proficiencies that information security professionals use in their jobs every day. Visit **sans.org/netwars**

Contact your sales representative to discuss a customized training and recruitment plan to ensure that your security team is capable and prepared.

support@sans.org
301-654-SANS (7267)

Extend and Validate Your Training

Combine the Flexibility of **Online Training** with the Power of **GIAC Certification**

Special Pricing

SANS ONLINE TRAINING

Convenience and Flexibility

SANS Online Training offers several convenient training options to fit your learning style. Whether you are interested in anytime, anywhere access, live streaming from a SANS classroom, or live streaming during the evenings directly from your instructor, the flexibility of SANS Online Training will allow you to learn the skills necessary to prepare for GIAC Certification Exams.

With **SANS OnDemand**, **SANS Simulcast**, and **SANS vLive**, you'll get:

- Content that Helps You Rewind, Revisit, Reinforce, and Retain in order to Help You Study for Your GIAC Exam and Retain Your SANS Knowledge Over the Long Term.
- Four or More Months of Access
- Same Instructors as Live Events
- Same Content as Live Events
- Same GIAC Certification Test Results

GIAC CERTIFICATIONS

Excellence and Capability

Broad, general InfoSec certifications are no longer enough: a SANS trained and GIAC certified workforce is necessary to combat today's cyber threats. That's because each GIAC certification focuses on specific job skills to ensure that professionals not only have the specialized knowledge to stay competitive in the marketplace, but also can defend and protect their organization/enterprise on day one.

Sign up for a GIAC Certification Attempt for only $799 when you add it during your Online Training course registration.

> **"Passed my @CertifyGIAC #GXPN this AM. What a great course! Glad I did the @SANSPenTest course #OnDemand. I rewatched the videos on advanced topics multiple times."** — **Mike Boya on Twitter**

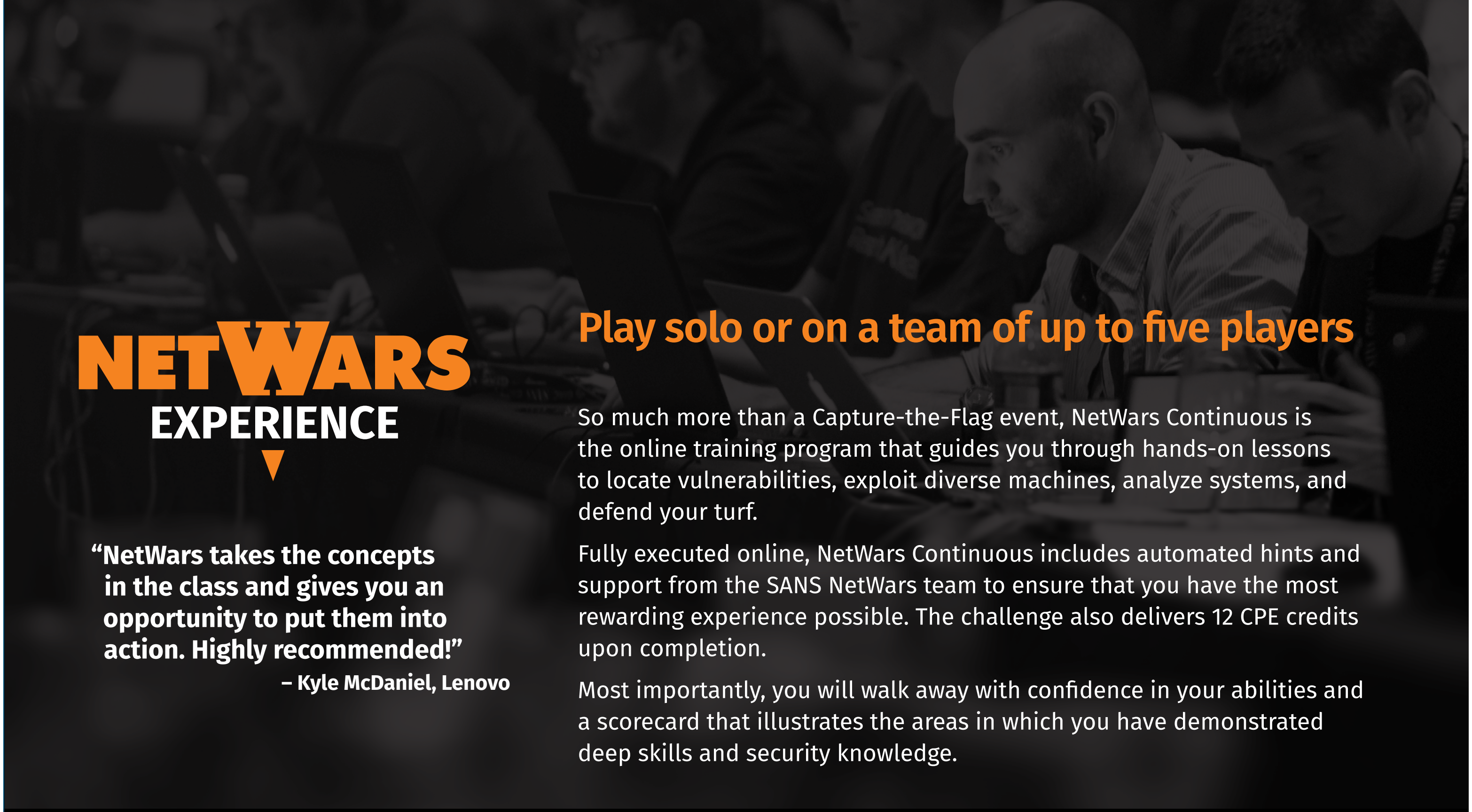
More information **sans.org/online | giac.org**

Upcoming Live Simulcast Events

For the full list of Simulcast courses, please visit **sans.org/simulcast**

		Simulcast from this event:
Austin 2019	Nov 18 - 23, 2019	4 Courses + NetWars
Pen Test HackFest 2019	Nov 20 - 25, 2019	7 Courses + NetWars
Cyber Defense Initiative 2019	Dec 12 - 17, 2019	10 Courses + NetWars
Miami 2020	Jan 13-18, 2020	4 Courses
Las Vegas 2020	Jan 27 - Feb 1, 2020	3 Courses
Security East 2020	Feb 3 - 8, 2020	12 Courses + NetWars

EXPERIENCE NETWARS CONTINUOUS



NETWARS EXPERIENCE

"NetWars takes the concepts in the class and gives you an opportunity to put them into action. Highly recommended!"

– Kyle McDaniel, Lenovo

Play solo or on a team of up to five players

So much more than a Capture-the-Flag event, NetWars Continuous is the online training program that guides you through hands-on lessons to locate vulnerabilities, exploit diverse machines, analyze systems, and defend your turf.

Fully executed online, NetWars Continuous includes automated hints and support from the SANS NetWars team to ensure that you have the most rewarding experience possible. The challenge also delivers 12 CPE credits upon completion.

Most importantly, you will walk away with confidence in your abilities and a scorecard that illustrates the areas in which you have demonstrated deep skills and security knowledge.

sans.org/netwars/continuous

Cyber Defense Essentials

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attackers work, and manage incidents as they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

SANS Cyber Defense Essentials courses help you build a solid foundation of core policies and practices to enable you and your security teams to practice proper incident response, then expand upon those crucial skills by adding advanced core techniques to help defend an enterprise from every angle.

Whether you're new to security or need a broad overview of security topics, these courses will support your effort to win the battle against the wide range of cyber adversaries that want to harm environments.

> **"OnDemand really worked for me. It allowed me to take my time to read the material, stop and find supplemental information if needed, and stop the lecture and repeat sections."**
>
> **- PATRICIA COHEN, Institute for Defense Analyses**

Stephen Sims
CDE – Curriculum Lead
SANS Fellow

Cyber Defense Essentials | Course List

	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
SEC301: **Introduction to Cyber Security** This introductory course is the fastest way to get up to speed in information security. The entry-level course includes a broad spectrum of security topics and real-life examples and can be used to prepare for GISF Certification. **www.sans.org/SEC301**	●	●	●	●	**GISF**
SEC401: **Security Essentials Bootcamp Style** In this course, students learn the language and underlying theory of computer and information security. Since all jobs today require an understanding of security, this course will help you understand how security applies to your job. In addition, students will gain the essential and latest knowledge and skills required for effective management of security systems and processes. **www.sans.org/SEC401**	●	●	●	●	**GSEC**
NEW! SEC402: **Cybersecurity Writing: Hack the Reader** Master the writing secrets that will make you stand out in the eyes of your peers, colleagues, managers, and clients. Learn to communicate your insights, requests, and recommendations persuasively and professionally. Make your cybersecurity writing remarkable. **www.sans.org/SEC402**	●			●	
SEC440: **Critical Security Controls: Planning, Implementing, and Auditing** This two-day course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security. These Critical Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. **www.sans.org/SEC440**	●			●	
SEC501: **Advanced Security Essentials – Enterprise Defender** A key theme of this course is that prevention is ideal, but detection is a must. Security professionals must know how to constantly advance security efforts in order to prevent as many attacks as possible. This prevention needs to occur both externally and internally via portable, network and server environments. **www.sans.org/SEC501**	●	●	●	●	**GCED**
SEC566: **Implementing and Auditing the Critical Security Controls – In-Depth** As threats evolve, an organization's security should evolve as well. To enable your organization to stay on top of this ever-changing scenario, SANS designed this course to train students how to implement the Twenty Critical Security Controls – a prioritized, risk-based approach to security that was designed by a master group of private and public sector experts from around the world. **www.sans.org/SEC566**	●	●	●	●	**GCCC**
SEC599: **Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses** This course provides an in-depth understanding of how current adversaries operate and arms you with the knowledge and expertise you need to detect and respond to today's threats. SEC599 aims to leverage the purple team concept by bringing together red and blue teams for maximum effect. The course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. **www.sans.org/SEC599**	●	●	●	●	**GDAT**

SEC599 & Purple Team

Although they share a common goal, Blue (defensive) and Red (offensive) Teams are not always well-aligned, which leads to most organizations not leveraging the full value of their teams' overall expertise. The respective teams typically report to a different hierarchy, which leads to different objectives:

BLUE TEAM – DEFENSE	RED TEAM – OFFENSE
1. Implementing Controls	1. Vulnerability Assessments
2. Security Monitoring	2. Penetration Tests
3. Incident Response	3. Adversary Emulation

The Purple Team concept brings Red and Blue together, encouraging the two teams to share insight and feedback to achieve one common goal.

THE PURPLE TEAM COMMON GOAL

To improve an organization's security posture.

Through real-world examples and lab exercises, SEC599 illustrates what adversaries are actually doing now, and how we can effectively combat their tactics using a Kill Chain structure.

Blue Team Operations

SANS Blue Team Operations courses teach you the critical skills required to defend your organization against cyber-attacks and improve its overall security posture.

The term Blue Team comes from the world of military simulation exercises. During exercises, the Red Team plays the role of the adversary (Offense), and the Blue Team acts as the friendly forces being attacked (Defense). Specifically emphasizing cybersecurity, the Blue Team's focus is to defend the organization from digital/cyber attacks. To be Blue Team means developing and implementing multiple security controls in a layered defense-in-depth strategy, verifying their effectiveness, and continuously monitoring and improving defenses.

In theory, everything that improves defensive security posture could be classified as Blue Team, but true Blue Team Operations imply that there is an overt emphasis on discovering and defending against attacks. Security professionals must have intimate knowledge of their existing environments to assess their current states and attacks against them.

SANS Blue Team Operations courses give you the knowledge, tools, and techniques needed to defend your networks with insight and awareness. The courses help you implement a modern security design that allows you to defend networks and understand threats. Monitoring and detection education includes learning to build the network and endpoint security, then carefully navigate through automation and Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM).

Seth Misenar
Blue Team Operations
Co-Curriculum Lead
SANS Fellow

Eric Conrad
Blue Team Operations
Co-Curriculum Lead
SANS Fellow

Blue Team Operations | Course List

	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
NEW! SEC450: **Blue Team Fundamentals: Security Operations and Analysis** SEC450 is an accelerated on-ramp for new cyber defense team members and Security Operations Center managers. This course introduces students to the tools common to a defender's work environment, and packs in all the essential explanations of tools, processes, and data flow that every blue team member needs to know. **www.sans.org/SEC450**	●			●	
SEC455: **SIEM Design & Implementation** This course will teach you the required stages of log collection, endpoint agent selection, logging formats, parsing, enrichment, storage, and alerting, as well as how to combine these components to make a flexible, high-performance SIEM solution. **www.sans.org/SEC455**	●			●	
SEC487: **Open-Source Intelligence (OSINT) Gathering and Analysis** This course is an introduction to open-source intelligence that teaches skills, techniques, and tools that law enforcement, private investigators, cyber attackers, and defenders use to scour information across the Internet, analyze results, and pivot to find other areas for investigation. **www.sans.org/SEC487**	●	●	●	●	
SEC503: **Intrusion Detection In-Depth** This course teaches core knowledge, tools, and techniques that will help students who monitor and defend networks. Students will learn the theory of TCP/IP and popular application protocols like DNS and HTTP in order to intelligently examine network traffic for signs of intrusions. Hands-on practice includes open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. **www.sans.org/SEC503**	●	●	●	●	**GCIA**
SEC505: **Securing Windows and PowerShell Automation** In SEC505 students learn to defend against pass-the-hash attacks, administrator account compromise, and the lateral movement of hackers inside the network by implementing the Critical Security Controls and PowerShell in a Windows environment. **www.sans.org/SEC505**	●	●	●	●	**GCWN**
SEC506: **Securing Linux/Unix** SEC506 provides in-depth coverage of Linux and Unix security issues and examines how to mitigate or eliminate general problems that apply to all Unix-like operating systems. Specific configuration guidance and practical, real-world examples, tips, and tricks are provided to help students remove vulnerabilities. **www.sans.org/SEC506**	●			●	**GCUX**
SEC511: **Continuous Monitoring and Security Operations** The Defensible Security Architecture and Network Security Monitoring/Continuous Diagnostics and Mitigation/Continuous Security Monitoring taught in this course will best position your organization or Security Operations Center to analyze threats and detect anomalies that could indicate cybercriminal behavior. **www.sans.org/SEC511**	●	●	●	●	**GMON**
SEC530: **Defensible Security Architecture and Engineering** Establish and maintain a holistic and layered approach to security that balances detection, prevention, and response capabilities, with implementation of appropriate controls on the network. With a heavy focus on leveraging current infrastructure (and investment), students in this course will learn how to reconfigure devices to significantly improve their organizations' prevention capabilities in the face of today's dynamic threat landscape. **www.sans.org/SEC530**	●	●		●	**GDSA**
SEC545: **Cloud Security Architecture and Operations** This course takes you from A to Z in the cloud, with everything ranging from policy, contracts, and governance to controls at all layers. The course covers automation tactics that will help you work effectively with the DevOps teams and build a sustainable cloud security program in your environment. **www.sans.org/SEC545**	●			●	
SEC555: **SIEM with Tactical Analytics** This course is designed to guide the student through the steps of tailoring and deploying Security Information Event Management (SIEM) to full Security Operations Center (SOC) integration. The underlying theme is to actively apply continuous monitoring and analysis techniques by utilizing modern cyber threat attacks. Labs involve replaying captured attack data to provide real-world results and visualizations. **www.sans.org/SEC555**	●	●	●	●	**GCDA**

Penetration Testing

What makes SANS Penetration Testing courses special?

In SANS Penetration Testing courses, you will learn in-depth, hands-on skills associated with the most powerful and common attacks today.

- Penetration testers, vulnerability assessment personnel, and Red Teamers: You'll be able to apply your skills in your very next engagement, providing even more technical depth and business value.
- Cyber defenders and Blue Teamers: You'll gain key insights into offensive tactics that will help you significantly improve your organization's defenses.
- Forensic analysts and incident handlers: You'll transform your understanding of the adversary's methods and be better able to anticipate and counter the attacker's next move.

What is high-value penetration testing and why is it important? A high-value penetration test:

- Emulates the activities of real-world attackers
- Discovers vulnerabilities in target systems
- Exploits those vulnerabilities under controlled circumstances
- Applies technical excellence to determine and document risk and potential business impact
- Conducts professional and safe testing according to a carefully designed scope and rules of engagement
- Helps an organization with its goal of properly prioritizing resources
- Teaches skills that will help all cybersecurity professionals in their work of securing their organization.

> **"I've used several different platforms in the past and NONE have been so well put together as SANS OnDemand. I could go on and on about what I like about the interface and how well the material goes with the book and the labs go with both. Programmers, well done!"**
>
> **-—FRANCIS COLVAIS, PYA**

Stephen Sims
Penetration Testing –
Curriculum Lead
SANS Fellow

Penetration Testing | Course List

	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
NEW! SEC460: **Enterprise Threat and Vulnerability Assessment** This course covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy from day one. The course is focused on equipping information security personnel responsible for securing 10,000 or more systems. **www.sans.org/SEC460**	●	●		●	**GEVA**
SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling** SEC504 will prepare you to turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. You will learn a time-tested, step-by-step process to respond to computer incidents; how attackers undermine systems so you can prepare, detect, and respond to them; and how to discover holes in your system before the bad guys do. **www.sans.org/SEC504**	●	●	●	●	**GCIH**
SEC542: **Web App Penetration Testing and Ethical Hacking** In SEC542, you will practice exploiting web applications to find flaws in your enterprise's web apps. Through hands-on exercises you will learn the four-step process for web application penetration testing; inject SQL into back-end databases to learn how attackers exfiltrate sensitive data; and utilize cross-site scripting attacks to dominate a target infrastructure. **www.sans.org/SEC542**	●	●	●	●	**GWAPT**
SEC560: **Network Penetration Testing and Ethical Hacking** SEC560 prepares you to conduct successful penetration testing and ethical hacking projects. The course will teach you how to perform detailed reconnaissance, exploit target systems to gain access and measure real business risk, and scan target networks using best-of-breed tools in hands-on labs and exercises. **www.sans.org/SEC560**	●	●	●	●	**GPEN**
SEC573: **Automating Information Security with Python** SEC573 will prepare you to apply Python coding skills. You will learn to tweak, customize, and develop your own tools to become a great penetration tester; develop applications that interact with networks, websites, databases, and file systems; and build practical applications that you can immediately put into use in your penetration tests. **www.sans.org/SEC573**	●	●		●	**GPYC**
SEC575: **Mobile Device Security and Ethical Hacking** SEC575 will prepare you to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills required to protect and defend mobile device deployments. **www.sans.org/SEC575**	●	●		●	**GMOB**
NEW! SEC580: **Metasploit Kung Fu for Enterprise Pen Testing** SEC580 will show students how to apply the incredible capabilities of the Metasploit Framework in a comprehensive penetration testing and vulnerability assessment regimen, and according to a thorough methodology for performing effective tests. **www.sans.org/SEC580**	●			●	
SEC617: **Wireless Penetration Testing and Ethical Hacking** SEC617 is designed for professionals seeking a comprehensive technical ability to understand, analyze, and defend the various wireless technologies that have become ubiquitous in our environments and, increasingly, key entrance points for attackers. You'll receive the SANS Wireless Assessment Toolkit (SWAT), a collection of hardware and software tools to jumpstart your ability to assess wireless systems. **www.sans.org/SEC617**	●			●	**GAWN**
SEC642: **Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques** SEC642 will teach you the advanced skills and techniques required to test modern web applications and next-generation technologies. In this course, you will learn the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing applications. The course concludes with an intensive hands-on Capture-the-Flag challenge where you will apply the knowledge you have acquired throughout the course in a fun environment, based on real-world technologies. **www.sans.org/SEC642**	●	●	●	●	

Rob Lee
Digital Forensics and Incident
Response Curriculum Lead
SANS Fellow

Digital Forensics and **Incident Response**

With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime. Adversaries are no longer compromising one or two systems in enterprises; they are compromising hundreds. Organizations of all sizes need personnel who can master incident response techniques to properly identify compromised systems, provide effective containment of the breach, and rapidly remediate the incident. Likewise, government and law enforcement agencies require skilled personnel to perform media exploitation and recover key evidence available on adversary systems and devices.

SANS DFIR courses will teach you to:

- Hunt for the adversary before and during an incident across your enterprise
- Acquire in-depth digital forensics knowledge of the Microsoft Windows and Apple OSX operating systems
- Examine portable smartphone and mobile devices to look for malware and digital forensic artifacts
- Incorporate network forensics into your investigations, providing better findings, and getting the job done faster
- Leave no stone unturned by incorporating memory forensics into your investigations
- Understand the capabilities of malware to derive threat intelligence, respond to information security incidents, and fortify defenses
- Identify, extract, prioritize, and leverage cyber threat intelligence from advanced persistent threat (APT) intrusions
- Recognize that a properly trained incident responder could be the only defense an organization has during a compromise

> **"SANS has created such an outstanding learning environment. Whether through its online or in-person training, the instructors and the content are far superior to anything else I have experienced. Keep up the great work."**
>
> **— ADAM FOWLER, GMAC**

DFIR | Course List

Course	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
NEW! FOR498: **Battlefield Forensics & Data Acquisition** This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly identify, collect, preserve, and respond to preserve data from a wide range of storage devices and repositories, ensuring that the integrity of the evidence is beyond reproach. **www.sans.org/FOR498**	●			●	
FOR500: **Windows Forensic Analysis** In FOR500, you'll learn to build in-depth and comprehensive digital forensics knowledge of Microsoft Windows operating systems by analyzing and authenticating forensic data, as well as track detailed user activity and organize findings. **www.sans.org/FOR500**	●	●	●	●	**GCFE**
FOR508: **Advanced Incident Response, Threat Hunting, and Digital Forensics** This course teaches advanced skills to hunt, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivists. You'll use threat hunting to catch intrusions in progress, instead of after attackers have attained their objectives. **www.sans.org/FOR508**	●	●	●	●	**GCFA**
FOR518: **Mac and iOS Forensic Analysis and Incident Response** This course provides intense hands-on forensic analysis and incident response skills to enable analysts to broaden their capabilities and gain the confidence and knowledge to comfortably analyze any Mac or iOS device. In addition to traditional investigations, the course presents intrusion and incident response scenarios to help analysts learn ways to identify and hunt down attackers that have compromised Apple devices. **www.sans.org/FOR518**	●	●		●	
FOR526: **Advanced Memory Forensics & Threat Detection** In this course, we'll dig into memory and uncover the malicious code where it runs. Security analysts need critical analysis skills to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work in order to tackle advanced forensics, trusted insider, and incident response cases. **www.sans.org/FOR526**	●	●		●	
FOR572: **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** This course covers the tools, technology, and processes required to integrate network data sources into your investigations, with a focus on efficiency and effectiveness. There are many use cases for network data, including proactive threat hunting, reactive forensic analysis, and continuous incident response. Learn the techniques that can help close gaps in these use cases and dive into the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. **www.sans.org/FOR572**	●	●	●	●	**GNFA**
FOR578: **Cyber Threat Intelligence** During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team to counter the threat. This course teaches the tactical, operational, and strategic level of cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, security operations more robust, and organizations more aware of the evolving threat landscape. **www.sans.org/FOR578**	●	●	●	●	**GCTI**
FOR585: **Smartphone Forensic Analysis In-Depth** In FOR585, you'll develop advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from smartphones. The course provides specialized training on how to analyze different file systems and artifacts from smart devices, leveraging a variety of forensic tools as well as custom scripts and queries to uncover hidden data often crucial to the success of an investigation. **www.sans.org/FOR585**	●	●	●	●	**GASF**
FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** This course equips students with the skills necessary to methodically analyze malicious software, acting as a practical on-ramp for the professionals wanting to expand their skills in this area. Attendees will learn how to perform interactive behavioral analysis of malware, deobfuscate samples, circumvent anti-analysis capabilities, and review key aspects of malicious code for a deeper understanding of its functionality. **www.sans.org/FOR610**	●	●	●	●	**GREM**

Additional Courses

Management Curriculum

Course	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
MGT414: **SANS Training Program for CISSP® Certification** Prepares you to pass the current CISSP® certification exam. This is an accelerated course that assumes the student has an understanding of networks and operating systems, and focuses on the eight domains of knowledge as determined by (ISC)^2. **www.sans.org/MGT414**	●	●	●	●	GISP
MGT433: **SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program** Learn key concepts and skills to establish a mature security awareness program that turns your biggest risk into your greatest asset. SSAP Credential. **www.sans.org/MGT433**	●			●	
MGT512: **Security Leadership Essentials for Managers** This course is designed to empower managers who want to learn quickly on InfoSec issues and terminology. Learn security and how to manage security. **www.sans.org/MGT512**	●			●	GSLC
MGT514: **IT Security Strategic Planning, Policy, and Leadership** Be a security business leader who builds and executes strategic plans that resonate with other business executives, creates effective information security policy, and develops management skills to better lead, inspire, and motivate teams. **www.sans.org/MGT514**	●			●	GSTRT

Audit Curriculum

Course	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
AUD507: **Auditing and Monitoring Networks, Perimeters, and Systems** This course provides a risk-driven method to design an enterprise security-validation program. It covers a variety of high-level audit issues and general audit best practices. **www.sans.org/AUD507**	●	●		●	GSNA

Legal Curriculum

Course	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
LEG523: **Law of Data Security and Investigations** This course teaches the law of business, contracts, fraud, crime, IT security, IT liability and IT policy – with a focus on electronically stored and transmitted records. Investigators will learn how to prepare reports, whether for cyber crimes, forensics, incident response, human resources or other investigations. **www.sans.org/LEG523**	●	●	●	●	GLEG

DevSecOps Curriculum

Course	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
DEV522: **Defending Web Applications Security Essentials** Learn how to defend web applications that traditional network defenses like firewalls fail to secure. The quantity and importance of data entrusted to web applications is growing and defenders need to learn how to secure those data. **www.sans.org/DEV522**	●	●		●	GWEB
SEC534: **Secure DevOps: A Practical Introduction** Ths course explains the fundamentals of DevOps, and how teams can build and deliver secure software. Learn how to leverage the principles, practices and tools to improve the reliability, integrity and security of systems. **www.sans.org/SEC534**	●			●	
SEC540: **Cloud Security and DevOps Automation** Master the tools needed to build and deliver secure software using DevOps and cloud services, specifically Amazon Web Services (AWS). Explore how the principles, practices, and tools of DevOps and AWS can improve the reliability, integrity, and security of applications. **www.sans.org/SEC540**	●	●		●	GCSA

Industrial Control Systems Curriculum

Course	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS
ICS410: **ICS/SCADA Security Essentials** This course is designed to train the workforce involved in supporting and defending industrial control systems on how to keep the operational environment safe, secure, and resilient against current and emerging threats. **www.sans.org/ICS410**	●	●		●	GICSP
ICS515: **ICS Active Defense and Incident Response** Deconstruct ICS cyber attacks, leverage an active defense to identify and counter threats in your ICS, and maintain the safety and reliability of operations. This course will help you understand your networked ICS environment, monitor it for threats, perform incident response against identified threats, and learn from interactions to enhance network security. **www.sans.org/ICS515**	●			●	GRID

Course Pricing

Cyber Defense

		ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY	GIAC CERTIFICATIONS	2020 PRICE
	SEC301: **Introduction to Cyber Security**	•	•	•	•	GISF	$6,090
	SEC401: **Security Essentials Bootcamp Style**	•	•	•	•	GSEC	$7,020
NEW!	SEC402: **Cybersecurity Writing: Hack the Reader**						$2,800
	SEC440: **Critical Security Controls: Planning, Implementing, and Auditing**	•			•		$2,800
NEW!	SEC450: **Blue Team Fundamentals: Security Operations and Analysis**						$7,020
	SEC455: **SIEM Design & Implementation**	•			•		$2,800
	SEC487: **Open-Source Intelligence (OSINT) Gathering and Analysis**	•	•	•	•		$7,020
	SEC501: **Advanced Security Essentials – Enterprise Defender**	•	•	•	•	GCED	$7,020
	SEC503: **Intrusion Detection In-Depth**	•	•	•	•	GCIA	$7,020
	SEC505: **Securing Windows and PowerShell Automation**	•	•	•	•	GCWN	$7,020
	SEC506: **Securing Linux/Unix**	•			•	GCUX	$7,020
	SEC511: **Continuous Monitoring and Security Operations**	•	•	•	•	GMON	$7,020
	SEC530: **Defensible Security Architecture and Engineering**	•	•		•	GDSA	$7,020
	SEC545: **Cloud Security Architecture and Operations**	•			•		$6,090
	SEC555: **SIEM with Tactical Analytics**	•	•	•	•	GCDA	$7,020
	SEC566: **Implementing and Auditing the Critical Security Controls – In-Depth**	•	•	•	•	GCCC	$6,090
	SEC599: **Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses**	•	•	•	•	GDAT	$7,020

Penetration Testing

NEW!	SEC460: **Enterprise Threat and Vulnerability Assessment**	•	•		•	GEVA	$7,020
	SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**	•	•	•	•	GCIH	$7,020
	SEC542: **Web App Penetration Testing and Ethical Hacking**	•	•	•	•	GWAPT	$7,020
	SEC560: **Network Penetration Testing and Ethical Hacking**	•	•	•	•	GPEN	$7,020
	SEC573: **Automating Information Security with Python**	•	•		•	GPYC	$7,020
	SEC575: **Mobile Device Security and Ethical Hacking**	•	•		•	GMOB	$7,020
NEW!	SEC580: **Metasploit Kung Fu for Enterprise Pen Testing**						$2,640
	SEC617: **Wireless Penetration Testing and Ethical Hacking**	•			•	GAWN	$7,020
	SEC642: **Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques**	•	•	•	•		$7,020
	SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**	•			•	GXPN	$7,020

Incident Response & Forensics

NEW!	FOR498: **Battlefield Forensics & Data Acquisition**						$7,020
	FOR500: **Windows Forensic Analysis**	•	•	•	•	GCFE	$7,020
	FOR508: **Advanced Incident Response, Threat Hunting, and Digital Forensics**	•	•	•	•	GCFA	$7,020
	FOR518: **Mac and iOS Forensic Analysis and Incident Response**	•	•		•		$7,020
	FOR526: **Advanced Memory Forensics & Threat Detection**	•	•		•		$7,020
	FOR572: **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**	•	•	•	•	GNFA	$7,020
	FOR578: **Cyber Threat Intelligence**	•	•	•	•	GCTI	$6,090
	FOR585: **Smartphone Forensic Analysis In-Depth**	•	•	•	•	GASF	$7,020
	FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**	•	•	•	•	GREM	$7,020

Security Management

	MGT414: **SANS Training Program for CISSP® Certification**	•	•	•	•	GISP	$7,020
	MGT433: **Securing The Human: How to Build, Maintain, and Measure a High-Impact Awareness Program**	•			•		$2,800
	MGT512: **Security Leadership Essentials for Managers**	•			•	GSLC	$6,600
	MGT514: **IT Security Strategic Planning, Policy, and Leadership**	•			•	GSTRT	$6,600

DevSecOps

	DEV522: **Defending Web Applications Security Essentials**	•	•		•	GWEB	$7,020
	SEC534: **Secure DevOps: A Practical Introduction**	•			•		$2,800
	SEC540: **Cloud Security and DevOps Automation**	•	•		•	GCSA	$6,600

Audit

	AUD507: **Auditing & Monitoring Networks, Perimeters, and Systems**	•	•		•	GSNA	$7,020

Legal

	LEG523: **Law of Data Security and Investigations**	•	•	•	•	GLEG	$6,090

Industrial Control Systems

	ICS410: **ICS/SCADA Security Essentials**	•	•		•	GICSP	$7,020
	ICS515: **ICS Active Defense and Incident Response**	•			•	GRID	$7,020

Compare SANS Online

Platform Features

	ONDEMAND	SIMULCAST	VLIVE	SELFSTUDY
Voucher Credits May Be Applied to Course Fees	●	●	●	●
No Travel Cost	●	●	●	●
Minimal Impact on Your Normal Routine	●	●	●	●
Flexible & Effective SANS Training from Your Own Computer	●	●	●	●
Earn CPEs	●	●	●	●
Taught by an Unparalleled Faculty of Information Security Leaders	●	●	●	●
Same Courseware as Live SANS Training, Including Books, Media, and Exercises	●	●	●	●
Proprietary E-Learning Platform Available for 4 Months	●			
Live Evening Sessions for 5 or 6 Weeks			●	
Live Daytime One-Week Courses Streamed from SANS Live Events		●		
Integrated Quizzes to Reinforce Learning	●			
Subject-Matter-Expert Support via Live Chat and Email	●	●	●	●
Real-Time Access to Instructors		●	●	
Virtual Lab Access	4 Mo.	4 Mo.	6 Mo.	4 Mo.
Archived Live Course Recordings		4 Mo.	6 Mo.	

GIAC CERTIFICATIONS **Prove Your Skills | Stay Competitive | Get GIAC Certified**

SANS Online Training is ideal preparation for GIAC Certification Exams

Rewind and revisit content and take advantage of subject-matter-expert support to help you with complex topics and questions as you prepare for the GIAC Exam.

38 Specialized certifications available

> "GIAC defines a higher level of mastery and skill that is required in order to earn the credential. GIAC really stands out among other security certifications."
>
> —JOSH RINGER, BENFIS HEALTH SYSTEM

Learn more at **giac.org**

Securing **Approval** and **Budget** for Training

Packaging matters

Write a formal request

- All organizations are different, but because training requires a significant investment of both time and money, most successful training requests are made via a written document (short memo and/or a few powerpoint slides) that justifies the need and benefit. Most managers will respect and value the effort.
- Provide all the necessary information in one place. In addition to your request, provide all the right context by including the summary pages on Why SANS?, the Training Roadmap, the instructor bio, and additional benefits available at our live events or online.

Clearly state the benefits

Be specific

- How does the course relate to the job you need to be doing? Place the particular course you wish to take into the context of the SANS Career Roadmap. Are you establishing baseline skills? Transitioning to a more focused role? Decision-makers need to understand the plan and context for the decision.
- Highlight specifics of what you will be able to do afterwards. Each SANS course description includes a section titled “You Will Be Able To.” Be sure to include this in your request so that you make the benefits clear. The clearer the match between the training and what you need to do at work, the better.

Set the context

Establish longer-term expectations

- Information security is a specialized career path within IT, with practices that evolve as attacks change. Because of this, organizations should expect to spend 6%-10% of salaries to keep professionals current and improve their skills. Training for such a dynamic field is an annual, per-person expense, and not a once-and-done item.
- Take a GIAC Certification exam to prove the training worked. Employers value the validation of learning that passing a GIAC exam offers. Exams are psychometrically designed to establish competency for related job tasks.
- Consider offering trade-offs for the investment. Many professionals build annual training expense into their employment agreements even before joining a company. Some offer to stay for a year after they complete the training.

FOR500.2
Windows Forensic Analysis
SANS DFIR
Core Windows Forensics I: Windows Registry

SANS The most trusted source for information security training, certification, and research

Cybersecurity

Job Roles | Skills | SANS Courses

Use the **Course Roadmap** Inside to Select a **Career Path** and to Create Your SANS Training Plan

SANS ONLINE TRAINING

Online Training Formats

OnDemand

OnDemand is a comprehensive e-learning platform that allows you to complete SANS training from anywhere in the world, at any time. More than 45 pre-recorded courses come with four months of online access to your course, plus audio lectures, quizzes, labs, and printed materials. Subject-matter experts are available throughout your study period, helping you to master a subject in all of its depth and complexity.

Simulcast

Simulcast courses are perfect for students who can't travel or prefer remote training. Simulcast includes live streamed content from a SANS event delivered directly to your home or office. All Simulcast courses include dedicated pre-event set-up support, live chat to interact with moderators and peers during the lectures, and four months of post-event access to archives and subject-matter-expert support.

vLive

vLive is a live evening classroom course format that gives you the structure and interaction of a live course, along with the flexibility and repetition of an online course. The course meets twice per week for six weeks and includes six months of access to all course recordings and materials, allowing vLive students to have the best of both live and online training.

SelfStudy

SelfStudy online training provides students with SANS course books, exercises, lecture MP3s, and quizzes for a self-paced learning experience.

OnDemand Bundles

Add the features of OnDemand to a SANS live course. If you plan to attend a one-week course at one of SANS Institute's many live events, consider adding an OnDemand Bundle to get extended access to the course archives, the custom e-learning platform to manage your progress, and continuous support from subject-matter experts.
sans.org/ondemand/bundles

Private Training

Custom training programs incorporating both live and online instruction can be built for almost any SANS course, and provide your team with a tailored experience, unique to your organization's size, location, and composition of learners.

To explore your options for custom, distributed, live and online workforce training from SANS, contact us at **privatetraining@sans.org** or visit **sans.org/private-training**

Build a High-Performing Security Organization

Based on extensive research and long-term global observations, SANS recommends three strategies for building an effective security group:

1 Use Practical Organizing Principles

Nearly all of your complex information security tasks and frameworks can be contained within four simple constructs, including building and maintaining defenses, monitoring and detecting intrusions, proactively self-assessing, and responding to incidents.

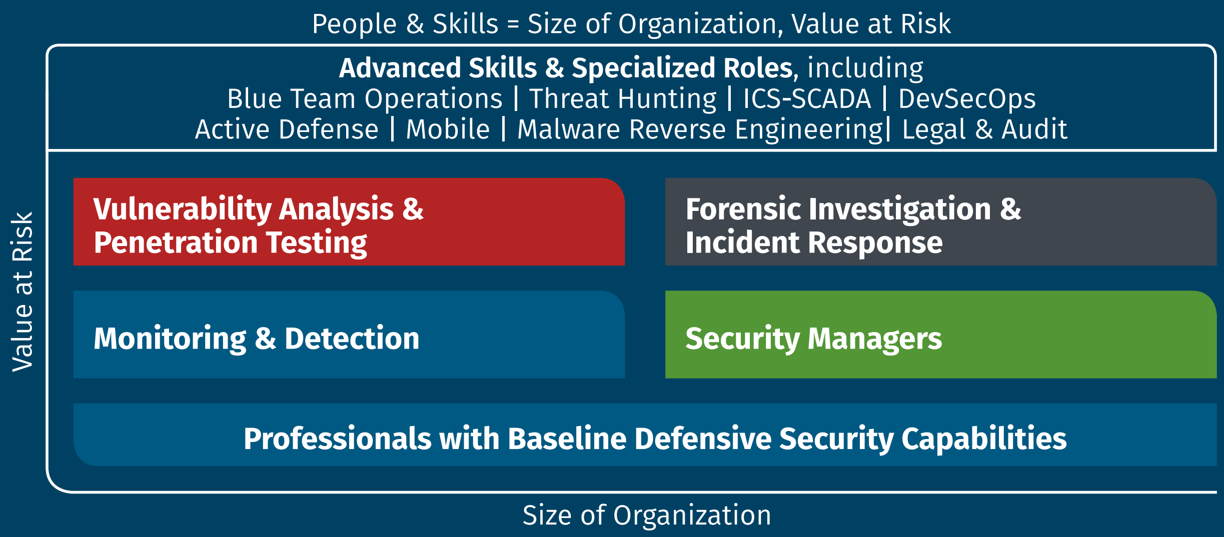
2 Implement Known Security Controls

Prioritize your efforts within your group framework using the Center for Internet Security's 20 Critical Security Controls. The Controls are a proven template for maturing your cybersecurity operations.

3 Evaluate and Empower Your People

Determine the number and type of professionals required to meet your organization's particular needs and address current threats (use the chart below as a guideline). Engage in an ongoing campaign to develop appropriate skills and capabilities in those professionals to defend your information. Cybersecurity is a critical and rapidly evolving practice area within IT that demands specialized training.

Best practice for building a high-performing security organization begins with ensuring baseline security skills for all, and having specialized professionals in offense, defense, and remediation who can effectively implement those practices.



People & Skills = Size of Organization, Value at Risk

Advanced Skills & Specialized Roles, including
Blue Team Operations | Threat Hunting | ICS-SCADA | DevSecOps
Active Defense | Mobile | Malware Reverse Engineering| Legal & Audit

Vulnerability Analysis & Penetration Testing

Forensic Investigation & Incident Response

Monitoring & Detection

Security Managers

Professionals with Baseline Defensive Security Capabilities

Value at Risk

Size of Organization

Get more detail about SANS training, instructors, and certifications by visiting our online, interactive roadmap at **sans.org/roadmap**. If you eed assistance in planning your team's future training, contact SANS at **info@sans.org** or **301-654-SANS (7267)**

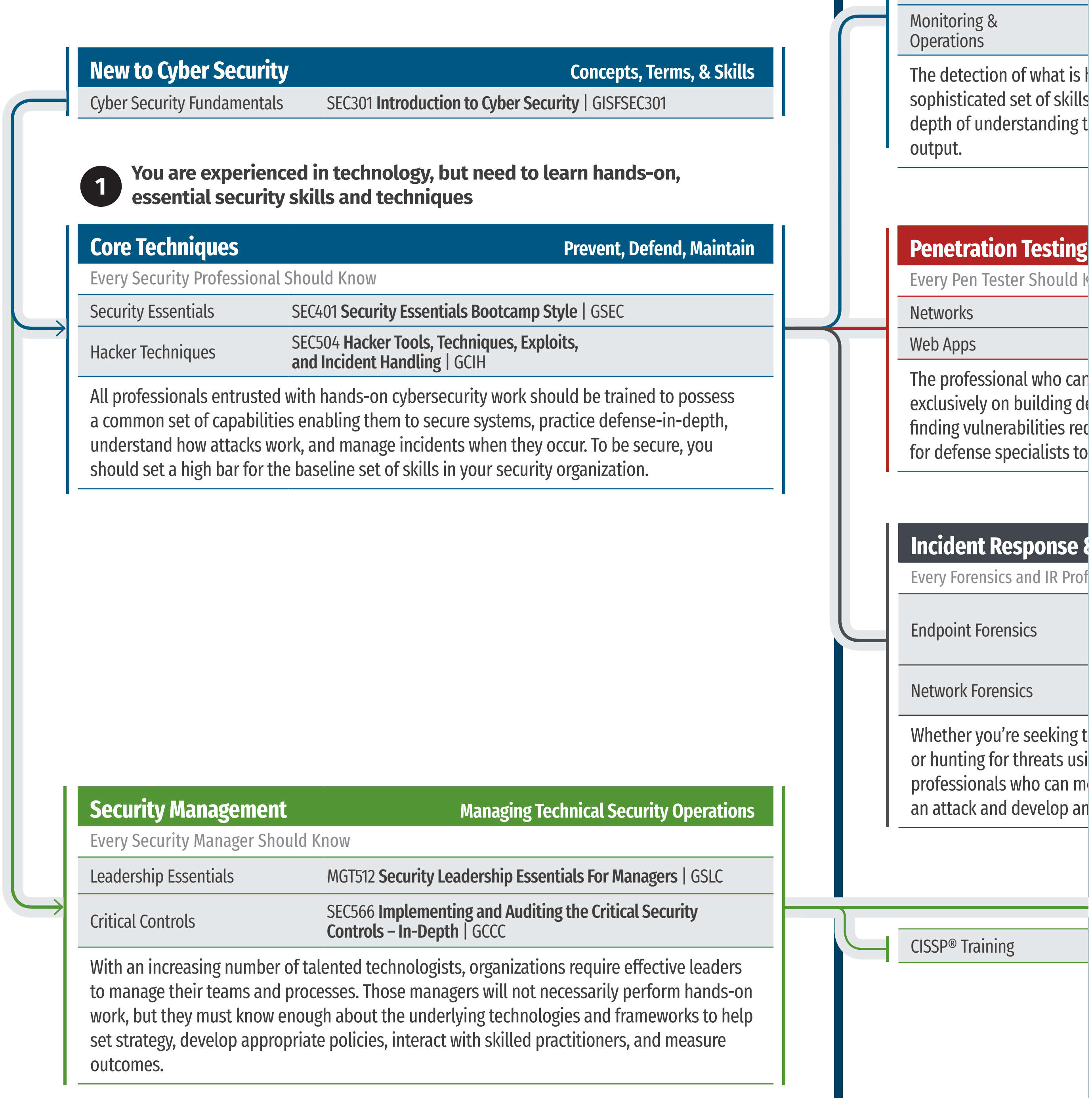
SANS The most trusted source for information security training, certification, and research

Baseline Skills

COURSE LISTING KEY:

Topic	Course Code	GIAC Certification
Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP	

Course Title



New to Cyber Security

Concepts, Terms, & Skills

Cyber Security Fundamentals	SEC301 **Introduction to Cyber Security** | GISFSEC301

1 **You are experienced in technology, but need to learn hands-on, essential security skills and techniques**

Core Techniques

Prevent, Defend, Maintain

Every Security Professional Should Know

Security Essentials	SEC401 **Security Essentials Bootcamp Style** | GSEC
Hacker Techniques	SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling** | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense-in-depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

Security Management

Managing Technical Security Operations

Every Security Manager Should Know

Leadership Essentials	MGT512 **Security Leadership Essentials For Managers** | GSLC
Critical Controls	SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Focus Job Rol

2 **You are experien for a specialized**

Monitoring & Detec

Scan Packets & Networks

Intrusion Detection

Monitoring & Operations

The detection of what is h sophisticated set of skills depth of understanding t output.

Penetration Testing

Every Pen Tester Should K

Networks

Web Apps

The professional who can exclusively on building de finding vulnerabilities red for defense specialists to

Incident Response &

Every Forensics and IR Prof

Endpoint Forensics

Network Forensics

Whether you're seeking t or hunting for threats usi professionals who can m an attack and develop an

CISSP® Training

es

nced in security, preparing
d job role or focus

tion — Intrusion Detection, Monitoring Over Time

SEC503 **Intrusion Detection In-Depth** | GCIA

SEC511 **Continuous Monitoring and Security Operations** | GMON

happening in your environment requires an increasingly s and capabilities. Identifying security anomalies requires increased o deploy detection and monitoring tools and to interpret their

Vulnerability Analysis, Ethical Hacking

Know

SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN

SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT

find weakness is often a different breed than one focused efenses. A basic tenet of red team/blue team deployments is that quires a different way of thinking, and different tools, but is essential improve their defenses.

& Threat Hunting — Host & Network Forensics

essional Should Know

FOR500 **Windows Forensic Analysis** | GCFE
FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA

FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

o maintain a trail of evidence on host or network systems, ng similar techniques, larger organizations need specialized ove beyond first-response incident handling in order to analyze appropriate remediation and recovery plan.

MGT414 **SANS Training Program for CISSP® Certification** | GISP

Crucial Skills, Specialized Role

3 You are a candidate for specialized or advanced tra

Cyber Defense Operations

Specialized Defensive Area

Blue Team	SEC450 **Blue Team Fundamentals: Security O**
OSINT	SEC487 **Open-Source Intelligence (OSINT) Ga**
Advanced Generalist	SEC501 **Advanced Security Essentials – Enter**
Cloud Security	SEC545 **Cloud Security Architecture and Ope**
Windows/Powershell	SEC505 **Securing Windows and PowerShell A**
Linux/ Unix Defense	SEC506 **Securing Linux/Unix** | GCUX
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA

Other Advanced Defense Courses

Security Architecture	SEC530 **Defensible Security Architecture** | GI
Adversary Emulation	SEC599 **Defeating Advanced Adversaries – Pu**

Specialized Penetration Testing

In-Depth Coverage

Vulnerability Assessment	SEC460 **Enterprise Threat and Vulnerability A**
Networks	SEC660 **Advanced Penetration Testing, Explo** SEC760 **Advanced Exploit Development for P**
Web Apps	SEC642 **Advanced Web App Testing, Ethical H**
Mobile	SEC575 **Mobile Device Security and Ethical H**
Wireless	SEC617 **Wireless Penetration Testing and Eth**
Hands-On Ranges	SEC562 **CyberCity Hands-on Kinetic Cyber Ra**
Python Coding	SEC573 **Automating Information Security wit**

Digital Forensics, Malware Analysis, & Threat Intel

Malware Analysis

Planning, Policy, Leadership	FOR610 **Reverse-Engineering Malware: Malw**

Threat Intelligence

Cyber Threat Intelligence	FOR578 **Cyber Threat Intelligence** | GCTI

Digital Forensics & Media Exploitation

Smartphones	FOR585 **Smartphone Forensic Analysis In-De**
Memory Forensics	FOR526 **Advanced Memory Forensics & Threa**
Mac Forensics	FOR518 **Mac and iOS Forensic Analysis and In**

Advanced Management

Management Skills

Planning, Policy, Leadership	MGT514 **Security Strategic Planning, Policy, a**
Project Management	MGT525 **IT Project Management, Effective Co**

Audit & Legal

Audit & Monitor	AUD507 **Auditing and Monitoring Networks,**
Law & Investigations	LEG523 **Law of Data Security and Investigati**

Training Roadmap | Development Paths

s

ining

SANS comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

Harden Specific Defenses

perations and Analysis

thering and Analysis

rprise Defender | GCED

rations

utomation | GCWN

DSA

rple Team Tactics and Kill Chain Defenses | GDAT

Focused Techniques & Areas

Assessment | GEVA

oit Writing, and Ethical Hacking | GXPN
Penetration Testers

Hacking, and Exploitation Techniques

acking | GMOB

ical Hacking | GAWN

nge Exercise

h Python | GPYC

Specialized Investigative Skills

ware Analysis Tools and Techniques | GREM

epth | GASF

at Detection

ncident Response

Advanced Leadership, Audit, Legal

nd Leadership | GSTRT

mmunication, and PMP® Exam Prep | GCPM

Perimeters & Systems | GSNA

ons | GLEG

Industrial Controls

Every ICS Security Professionals Should Know	
Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP
ICS Defense & Response	ICS515 **ICS Active Defense and Incident Response** | GRID
NERC Protection	
NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

DevSecOps

Every Developer Should Know	
Secure Web Apps	DEV522 **Defending Web Applications Security Essentials** | GWEB
Secure DevOps	SEC540 **Cloud Security and DevOps Automation** | GCSA

See in-depth course descriptions and the digital version of this roadmap at: **sans.org/roadmap**

To learn more about additional SANS courses, go to: **sans.org/courses**

These SANS courses are all currently available online except for SEC760, for up-to-date course information visit: **sans.org/online**

sans.org

SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

AFCEA
Corporate Member

As the leading provider of information defense, security, and intelligence training to military, government, and industry groups, the SANS Institute is proud to be a Corporate Member of the AFCEA community.

SANS ONLINE TRAINING

Test Drive over 45 SANS Cybersecurity Courses

The SANS Institute's free demos, delivered via the SANS OnDemand platform, give you a close look at a course's content, pace, and features.

sans.org/demo

Exclusive Special Offers

Choose a **tablet**, **laptop**, or **course discount** offer with select OnDemand and vLive courses. For more details, visit **sans.org/online**

Rewind | Revisit | Reinforce | Retain